A Guide for Developers of Division Applications

Version 1

Submarine Directorate
IRM Support Services

31 August, 2001

TABLE OF CONTENTS

1. Purpose

The purpose of this document is to present the process for developers who wish to create or update custom applications for Team Submarine. This document describes the current Team Submarine computing environment and a projection of the environment under the Navy/Marine-Corp Intranet (NMCI).

Members of the Team Submarine community (application sponsors) may also find this document useful in technical negotiations with developers, helping to define contract proposals and delivery requirements.

2. SEA 92L6 Authority

Team Submarine Operating Instruction XXXX states that sponsors proposing new applications or upgrading existing applications for the Team Submarine network must notify SEA 92L6 of their intentions prior to the start of any system/application acquisition. This allows SEA 92L6 to:

- Coordinate and resolve application development issues such as architectural constraints and information assurance with SEA 00I
- Provide computing environment guidelines
- Plan for the support required when the application is ready for testing and deployment.

SEA 92L6 will provide developers with information on how to tailor their design to the NMCI computing environment and with a list of requirements for application acceptance. Approval must be sought from SEA 92L6, even when the proposal is to extend the functionality of an existing application.

SEA 92L6 will also act as facilitator in the communication process between the sponsor and developer, will lay out a comprehensive guide for the development process and life cycle support of the application, will provide templates for support documentation, and will act as an interface between SEA 00I and the sponsor/developer team.

Finally, an outline in the form of a checklist will be provided to facilitate tracking of tasks necessary to complete the designated process.

3. Application Development Process

Sponsors must contact SEA 92L6, Mark Dronfield by phone at (202) 781-1206 or by e-mail at dronfieldma@navsea.navy.mil, during the initial planning phase of application development or enhancement. SEA 92L6 will assign someone in the SEA 92L6 branch to serve as the technical point of contact (TPOC) for each application development project. The sponsor of each development project must meet with the TPOC to review the proposed development plan. Once the development plan has been reviewed and agreed upon by the TPOC, the sponsor and the developer, the TPOC will schedule future meetings with both the sponsor and developer to

ensure that no technical issues arise that will put the project in jeopardy. The TPOC will also meet with the developer as needed to support the development effort.

4. Application Development Procedure

During the initial meeting(s) between the sponsor and the TPOC to discuss the proposed application development or enhancement, a formal plan for the development will be worked out. The details of the development plan will vary according to the level of complexity of the development effort. The TPOC will provide templates for many of the deliverables in the development plan, and can assist in filling them out. Refer to Appendix B for a complete list of required documentation and the location of appropriate templates.

5. The Computing Environment

This document will refer to two types of applications: standard and division. Standard applications, like Microsoft Word, Excel, PowerPoint, Access and Outlook, are provided to all users by NAVSEA or NMCI. Division applications are developed, purchased, or acquired by individual offices within Team Submarine. SEA 92L6 provides limited support to division applications, and does not own or administer any necessary software licenses. Some division applications may need a standard application, such as Microsoft Access or Word, as a component part.

5.1 Overview

5.1.1 Current

Team Submarine’s computing environment consists of Pentium workstations connected over 100-base-T unshielded twisted pair cable to a local hub. Production Novell NetWare 5.x File Servers are located in the Main Computer Room (MCR) in building 197 of the Washington Navy Yard. The NetWare servers are connected over a 100-base-FX backbone. The backbone is connected through a 100-base-FX connection to the NAVSEA backbone, which is directly connected to the Internet. Team Submarine's network is protected with a firewall and router, which is inside the NAVSEA network. The NAVSEA network is protected with a firewall and router. The Team Submarine network is comprised of multiple offices in two separate buildings in the Washington Navy Yard (WNY), and several offices in Crystal City in Arlington, VA.

Most of Team Submarine's network is certified to process "NOFORN" (no access by foreign nationals). This accreditation requires that all Team Submarine offices communicate with each other without going over the NAVSEA backbone. In addition, dial-in access to the LAN is not permitted, except for retrieving e-mail from designated mail gateways. Developers and sponsors must work within Team Submarine spaces while maintaining their applications. Remote access to applications or data on the production server within TEAMSUB, whether over modem, LAN or Internet, is strictly forbidden.

An exception to the above exists for the PMS 404, PMS 415 and ASTO program offices in that the ACME server segment is designated UNCLASS.

5.1.2 NMCI

Team Submarine's computing environment consists of (at a minimum) NMCI workstations connected over 100-base-T unshielded twisted pair cable to a local hub. The current plan is that all desktop computers will be "locked down", meaning neither Division Applications nor users will be permitted to install any files on client computers, with the possible exception of browser plug-ins.

Production Windows 2000 Servers are located in the Main Computer Room (MCR) in building 197 at the Washington Navy Yard. The servers are connected over a 100-base-FX backbone. The backbone is connected through a 100-base-FX connection to the NMCI backbone, which is directly connected to the Internet. Team Submarine's network is protected with a firewall and router, which is inside the NAVSEA network. The NAVSEA network is protected with a firewall and router. The Team Submarine network is comprised of multiple offices in two separate buildings in the Washington Navy Yard (WNY), and several offices in Crystal City in Arlington, VA.

Team Submarine's network will remain labeled "NOFORN" (no access by foreign nationals). See Section 5.1.1 for details pertaining to the TEAMSUB and PMS 404 segments.

5.2 The NAVSEA Network -- Novell Netware

5.2.1 Current

The NAVSEA network consists of desktops, peripherals and the unclassified Local Area Network (LAN), for which operational support is provided by SEA 00I. File and print services are handled through a Novell NetWare 5.x network. Team Submarine is part of a larger NAVSEA Novell Directory Services (NDS) tree. Team Submarine manages several organizational units (OU) under the NAVSEA organization (O). The tree structure is well defined and fully operational. Team Submarine does not have administrator rights to the root of the NAVSEA tree. Any proposed enhancement that might require a change to the schema of the NAVSEA NDS structure must be approved by SEA 00I.

Novell Application Launcher (NAL), also known as Z.E.N.Works, is used to manage and install most division applications. Applications are stored in the NDS as objects. Users are made members of groups that are associated with division applications objects. NAL is used to install all applications on the workstation. Most division applications open through the NAL window. NALs are created by NAVSEA Advanced Systems Group (ASG) or their deputies. SEA 92L6 cannot create NAL objects.

PMS 404, PMS 415 and ASTO offices do not use Novell NetWare servers; they run in a strictly Windows NT 4.0 Service Pack 6a network. Applications for these offices must operate in Microsoft NT environments. Applications for all other Team Submarine offices must operate in NetWare NDS environments.

5.2.2 NMCI

File and print services are handled through Microsoft Windows 2000 Servers using Active Directory. Applications must operate under Microsoft Windows 2000.

At this time it is not known what type of application manager software will be used.

5.3 The NAVSEA Network – Windows NT Networking

5.3.1 Current

Team Submarine has its own minimal NT domain that is used for application support. SEA 92L6 and NAVSEA ASG control access to this domain. Some disk space may be available, but developers are encouraged to provide sufficient hardware for their own requirements. There is also an NT based web server which is available to developers for launching applications. The NT domain is managed through NDS for NT. This enables management and security through a single directory.

Applications should operate in both NetWare NDS and Microsoft NT environments. NetBEUI and Net BIOS (and IP tunneling) protocols are filtered by Team Submarine and NAVSEA routers. NT servers and applications must use IP as the network protocol.

5.3.2 NMCI

Windows 2000 Active Directory will be used.

5.4 Desktop Operating System

5.4.1 Current

Team Submarine has workstations running Windows 95, Windows 98 and Windows 2000. Novell's 32-bit IntraNetWare client connects workstations to the network. Our desktop systems will be migrated to Windows 2000 under NMCI. This is scheduled to happen in calendar year 2002.

Every attempt is made to ensure that workstation configurations and installations are tightly integrated, optimized, and controlled. Changes to workstation configurations undergo rigorous analysis and testing to ensure compatibility, functionality, and stability.

5.4.2 NMCI

Windows 2000 will be the standard desktop environment. See Appendix A for the complete listing of NMCI Gold Disk desktop software configuration.

5.4.3 Section 508 Compliance

NMCI is intended to make the naval service more efficient and productive by providing data, video and voice communications to link 350,000 workstations throughout the department. The proposal will comply with Section 508 of the Rehabilitation Act, which states requires that Federal agencies' electronic and information technology is accessible to people with disabilities.

5.5 Standard Applications

5.5.1 Current

Team Submarine applications standard on all workstations include Word, Excel and PowerPoint from either Microsoft Office 97 or 2000. Team Submarine uses a customized version of Delrina Formflow for Navy, DoD and NAVSEA forms. Select users have Microsoft Access as a standard application. Microsoft Project licenses are purchased by each division and distributed on an as needed basis.

5.5.2 NMCI

Under NMCI, only Microsoft Office 2000 Professional will be supplied via NMCI. See Appendix A for the complete current list of NMCI provided desktop software.

5.6 Internet Access

5.6.1 Current

All workstations are assigned dynamic IP addresses and are connected to the Internet. Team Submarine maintains its own intranet server (“Flasher”). All intranet servers located in Team Submarine must undergo a requirements analysis and have a security plan developed.

5.6.2 Both Current and NMCI

The NAVSEA firewall blocks all IP ports above 1024 unless a waiver is granted.

Important Note: Waivers are not granted by NAVSEA. They are granted by the office of the Department of the Navy CIO (DONCIO). Waivers are rare and very difficult to justify.

5.7 E-Mail Access

5.7.1 Current

On the NAVSEA LAN the standard e-mail program is Microsoft Outlook 97. E-mail is available to users remotely via Outlook Web Access (OWA). E-mail may also be accessed by dialing into the NAVSEA Exchange server from a home or laptop computer running Outlook 97, 98 or 2000.

5.7.2 NMCI

Microsoft Outlook 2000 will be the standard e-mail program. Dial-in and OWA access to e-mail will not be permitted. This decision is subject to change.

5.8 Remote Connectivity/Access

5.8.1 Current

Users may dial into the NAVSEA network using a Secure ID device. Some users have access to a virtual desktop through a terminal server, which is accessed from within a Citrix client window.

5.8.2 NMCI

The policy for remote connectivity has not been finalized.

6. Application Development Requirements

6.1 Required Development Applications and Platforms

6.1.1 Current and NMCI

Task Force Web (established by the Vice Chief of Naval Operations in December 2000) mandates that all Navy applications will be web-based by 2004. Because of the Navy's strong commitment to web-based applications, deployment of only very small applications that are not web-based will be allowed. An example of an acceptable non-web-based application would be a small Microsoft database shared within a single branch or division, which resides on a network-shared drive.

The use of third-party web components is restricted to those for which plug-ins are provided by NMCI. Plug-ins not on the list must be submitted to the ISF for evaluation. Confirmation from NMCI is not guaranteed. (see Appendix A)

New hardware will be examined and tested before being permanently connected to our intranet. Currently this is done by SEA 00I. Under NMCI, the Information Strike Force (ISF) will do this. If you are providing equipment as part of the contract with your sponsor, you will turn over title and transfer any warranties once the application is accepted. These will be turned over to ISF or SEA 92L6 depending on whether or not the application is classified as "legacy" and uses one or more ISF CLIN numbers. You will also provide all documentation, configuration disks, and accessories to SEA 92L6, unless a support agreement with your sponsor specifies that you are to keep them.

6.2 Security

6.2.1 Current

The Team Submarine Novell Network provides file system security. Team Submarine will create a single NDS user group for a division application. This group may have exclusive file system rights to an application subdirectory. Only specified members of the group will have access to the application. This level of security may be inadequate for some applications.

If a more stratified security plan is required, the application developer must provide it within the application. For instance, there are many applications where a few individuals manage the application, provide updates, perform edits, or access more sensitive data. The application developer must provide any required security levels within the application itself through user authentication.

6.2.2 Both Current and NMCI

An SSAA must be completed for all applications, and updated whenever a significant change is made to the application or its environment. SSAAs are submitted to the Information Assurance division in SEA 00I for approval. SEA 92L6 will provide developers with an SSAA template (see Appendix B).

6.3 Workstation Configuration Requirements

6.3.1 Current

Division applications may not use " TSR" (Terminate and Stay Resident) programs, or have any memory resident parts wherein the entire application or a portion of the application runs in memory keeping the application running even though the application window is closed. Division applications should not require any additions or modifications to configuration files such as the autoexec.bat or config.sys. Division applications are highly discouraged from adding their directories to the workstation PATH statements or adding SET parameters. Applications should be controlled internally, by an INI file or by adding keys to the registry.

6.3.2 NMCI

Any applications that install any files or make any changes to the Windows Registry on a PC must go through the NAVSEA integration phase. No ad hoc installations on a PC will be permitted.

6.4 Drive letters and Path Information.

6.4.1 Current

The file server directory structure is well established and conforms to NAVSEA standards. Applications should be written to be path independent. File Server names may change, applications may be moved from one server to another, or from one path to another. This should not affect the operation of the application as long as the user's icon or shortcut is appropriately modified. SEA 92L6 will be responsible for distributing most icons and shortcuts and workstation installations. SEA 92L6 uses a distribution tool (Novell Application Launcher) to deliver applications to each workstation. (See section 5.2.1)

Workstation directories and paths may also change. Team Submarine prefers for developers to create their own directory, and store all relevant files under that directory and subdirectories. Application files should be kept in a separate subdirectory from data files. Division applications

may create a single directory off of the root of the C: drive, or off of the C:\program files\. A developer can manage subdirectories as their requirement dictates.

Files that must be added to the Windows directory should have unique, identifiable names. Keys added to the Windows registry should be clearly named as part of that application. Sections added to SYSTEM.INI, WIN.INI or other Microsoft default INI files should be labeled with the application. Developers are encouraged to create and utilize their own INI files.

Team Submarine prefers to run division applications from a file server with a minimum of workstation components.

6.4.2 NMCI

Data should be stored on the users network drive, rather than on the local hard drive. Drive letters have not been established yet. Web-based applications should not write any files to the local drive other than in the temp directory.

6.5 Maintenance and Upgrades

6.5.1 Current

In almost all situations, the developer or application sponsor is responsible for maintaining division applications. Currently, if the application resides on a supported NAVSEA file server, SEA 00I will provide daily backup, UPS protection, and virus protection. The NAVSEA Help Desk will help users start their application, and diagnose infrastructure problems, such as printing or Internet access issues. Once the fault is determined to be internal to the program, the sponsor or developer must provide appropriate levels of support to resolve the issue.

6.5.2 NMCI

NMCI will provide backups, UPS and virus protection and upgrades for NMCI hosted software, hardware, etc. Upgrades to all legacy applications will be the responsibility of the sponsor and/or developer.

6.6 NMCI Compliance

All division applications must be certified for NMCI compliance at an NMCI testing facility prior to being made accessible to users.

6.7 Development and Testing

While SEA 92L6 will provide technical oversight and management for all development tasks, the actual development and testing of the application is the responsibility of the developer and the sponsor. Team Submarine will assist in the final testing of an application before it goes "live" to the users. Such testing is limited to verifying compliance with the requirements in section 4 of this document. Applications should be fully tested before being introduced into the Team

Submarine environment. There should be no obvious faults upon delivery. The application should be ready for acceptance and integration testing.

6.7.1 Current

SEA 92L6 has a testing facility in the Century II Building, Suite ML-120, Crystal City, Virginia.

6.7.2 NMCI

All applications will be required to undergo a certification process. This process is intended to certify that the application will operate correctly in the NMCI basic load (Gold Disk) environment, that it does not adversely impact other NMCI applications, and that it is compliant with all security requirements imposed by the DoN.

Sponsors are encouraged to utilize the pre-certification process. The ISF will assist the sponsor in the processes for pre-certifications:

- Processes and criteria for pre-certification/certification of applications;
- Facilities for testing with sufficient testing cells;
- System administration support for the testing operations; and
- Advisory assistance in the execution of the certification tests.

An example of the test scenario for participation would be:

- The ISF would contact the application owner and they would agree to a script development process and participation in the testing effort by the sponsor.
- The application sponsor would provide requirements for the application to the ISF.
- The ISF would create test scripts (with sponsor participation) and conduct the tests in ISF labs.
- The application sponsor would approve the output of those ISF tests and work with the ISF on any issues that developed during the testing.

6.8 Documentation

The Developer must provide Team Submarine with sufficient information to support the installation, deployment, and maintenance of the division application. In addition, SEA 00I and Team Submarine requires contact information from developers, and technical information about any third-party hardware and software that the product may use. SEA 00I will manage this information at the corporate level.

See Appendix B for more information on required product documentation.

6.9 User Training

The application developer or sponsor is responsible for training their user community. The sponsor is responsible for providing necessary training handouts and other user documentation.

6.10 End-User Support

6.10.1 Current

End user support should be negotiated with SEA 00I. In most instances, SEA 00I will accept responsibility for application launching, printing, saving, and closing. SEA 00I is also responsible for any standard application or service that the division application may use, such as Microsoft Word, or TCP/IP. Developers or sponsors are responsible for all other operational support.

6.10.2 NMCI

We are anticipating that, under NMCI, the following end-user support services will be provided:

- Provide onsite installation and preventative maintenance of equipment/electronic devices
- Interact with customer to ensure satisfaction
- Provide technical assistance on the repair of equipment/electronic devices
- Provide customer assistance with routine inquiries and problems such as software, hardware and network operations
- Respond to and diagnose problems through discussion with users
- Provide support to end-users for PC, server or mainframe application and hardware
- Resolve escalated problems
- Interact with network services, software systems engineering and/or applications development to restore service and/or identify and correct core problem

7. Product Documentation

The Developer must provide Team Submarine with sufficient information to support the installation, deployment, and maintenance of the division application. In addition, Team Submarine requires contact information from developers, and technical information about any third-party hardware and software that the product may use.

Appendix A -- NMCI

A.1. List of software included in NMCI Gold Disk

This list is current as of 1 May, 2001. It was provided by the NAVSEA HQ NMCI office.

- Internet Explorer 5.5 (NOTE: Internet Explorer will be default browser. The home page will be http://homeport and the proxy is port 80).
- Radia Client
- Netscape Communicator 4.76
- Windows Media Player 7
- Real Player 8
- WinZip 8
- Adobe Acrobat Viewer
- Remote Management Software
- Smart Card Support
- WRQ Reflections
    - TN3270 Client - IP 3270 Client
    - VT100 Emulation
    - X-Terminal
    - Microsoft *Word*
    - Microsoft *Excel*
    - Microsoft *PowerPoint*
    - Microsoft *Access*
    - Microsoft *Outlook 2000*
- Plugins
    - Macromedia Shockwave v 8.0
    - Flash Player 5.0
    - Apple QuickTime Movie and Audio Viewer v4.12
    - IPIX v6, 2,0,5
- Norton AV CE 7.5
- Axent Intruder Alert
- Axent Enterprise System Management
- the Tivoli agent

A.2. NMCI URLs

TEAMSUB	http://teamsub.navsea.navy.mil/nmci
EDS	http://www.eds.com/nmci/
NAVSEA	http://nmci.navsea.navy.mil
NAVAIR	https://nmci.navair.navy.mil/
SPAWAR	https://nmci.spawar.navy.mil

Appendix B – Requirements Checklist

NOTE: Templates of documents may be found on the TEAMSUB website

Required	Not required	Category	Task Description	Validated by:
		Tasks (SEA 92L6)		
			Provide Sponsors with Team Submarine Operating Instruction Document	
			Provide Guides for Sponsors and Developers of Division Applications	
			Review development plan and allocate appropriate SEA 92L6 resources	
			Assign a technical point of contact (TPOC) for the project	
		Tasks (TPOC, Sponsor, Developer)		
			Chart progress through regularly scheduled status meetings with developer	
			Perform acceptance testing	
			Perform pre-certification testing	
			Perform post-certification testing	
		Tasks (TPOC)		
			Check new requirements against existing requirements on file with SEA 00I	
			Establish formal plan for development	
			Determine milestones	
			Provide project checklist	
			Provide developer with current, accurate NMCI prerequisites	
			Provide architectural constraints and information assurance documentation	
			Provide templates for necessary documentation	

Required	Not required	Category	Task Description	Validated by:
			Provide a repository for completed documentation	
			Provide support for testing and deployment phase	
			Determine network and workstation configuration requirements	
			Examine and test new hardware	
		Tasks (Sponsor)		
			Notify SEA 92L6 prior to starting the development process	
			Sponsor/Developer kick off meeting to determine requirements	
			Establish justification for installation, deployment and maintenance of the proposed division application	
			Acquire source code and licenses	
			Develop user groups and permissions	
			Determine user training and support needs	
		Tasks (Developer)		
			Develop application in accordance with requirements and specifications	
			Devise appropriate testing environment and procedures	
			Develop training plan and materials	
			Provide titles and transfer warranties to SEA 92L6 for all equipment provided as part of the contract	
		Documentation		
			Detailed Plan Of Action and Milestones (POAM) including PDRs and CDRs	
			Concept of Operations (CONOPS)	
			Information Strike Force (ISF) certification	
			Requirements analysis	
			Functional analysis	

Required	Not required	Category	Task Description	Validated by:
			Use-case analysis	
			Provide documentation for printing, back-up, virus protection, and Internet access requirements	
			List of software development tools used	
			List of platforms and versions used	
			Licenses and documentation for development tools, Commercial Off-The-Shelf (COTS) and/or Government Off-The-Shelf (GOTS) used in the application	
			Online help	
			User manual/documentation, if any	
			Source code burned onto a CD	
			System Security Authorization Agreement (SSAA)	
			Application installation program	
			Application installation support documentation	
			Acceptance test scripts	
			NMCI certification test scripts	

Appendix C – Definitions of Terms

Navy/Marine-Corp Intranet (NMCI) - is a comprehensive, enterprise-wide initiative that will make the full range of network-based information services available to Sailors and Marines. NMCI will provide the Navy and Marine Corps with secure, universal access to integrated voice, video and data communications, pier-side connectivity to Navy vessels in port, and will link more than 360,000 desktops.

TPOC – the Technical Point of Contact is an individual from SEA 92L6 who will be assigned to the development project to assist with the interpretation and execution of requirements as specified in the Sponsor and Developer Guides.

NOFORN – a security designation which allows no access to the server by foreign nationals

Task Force Web – provides oversight in the effort to ensure that operational and business processes are conducted worldwide via interconnected and interoperable web-based IT systems

NMCI Internet Strike Force – is a team of industry experts partnering in the NMCI initiative. The Strike Force will assume the responsibility for providing all assets and services needed to ensure the transmission of voice, video and data across the Department of the Navy.